暗号化ツールを導入する（メール、SNS、保存データ、パソコンのデバイス）

JCA-NET セミナー

2024 年 10 月 26 日

小倉利丸

toshi@jca.apc.org

はじめに

21 日のセミナーに引き続き暗号化を特集します。これまでも暗号化ツールについては、何度か紹介してきました。ネットやパソコンなどを利用する際に、ほとんど自覚することなく暗号化が機能している場合もありますが、意識的に暗号化のツールを導入することが必要になる場合があります。今回は、ほとんど事前の予備知識なしに導入できるいくつかの暗号化のツールを中心に紹介します。メールや SNS については、エンド・ツー・エンド暗号化に対応しているサービスを使うことで容易に実現できる反面、これまで使ってきたサービスからの切り替えが必要になるという点がハードルになります。保存データの暗号化やハードディスクの暗号化では特別のソフトウェアの導入などの作業も必要になりますが、以前よりも導入しやすくなっています。

暗号化は、知識として知っているだけでは自分の通信のプライバシーを防御できません。実践が第一なのです。しかしまた、パソコンやネットを苦手とする人たちにとって、暗号化は取り組みにくい課題と感じられる結果として、セキュリティのリスクに晒されやすくなる傾向があるともいえます。こうした点を念頭に置きながら、苦手な皆さんがひとつでも暗号化ツールの導入を実現できるためのノウハウを提供するように工夫します。

このセミナーで使用しているオンライン会議室 Jitsi-meet もエンド・ツー・エンド暗号化での会議を行なえるようになっています。この点についても、実際に試してみる予定です。（これは今回は取り上げません）

グローバル暗号化デー 2024 声明

2024 年 10 月 20 日

強力な暗号化は、人々、人々の情報、そして通信をプライベートかつ安全に保つための重要な技術です。暗号化はオンライン上の信頼を支え、脆弱なコミュニティのメンバーを保護し、政府、企業、そして市民のデータを犯罪者やその他の悪意ある行為者から守ります。

しかし、一部の政府や組織は暗号化の弱体化を推し進めており、これは世界中の何十億もの人々のセキュリティとプライバシーを危険にさらす前例を作ることになります。暗号化を弱体化させるような一国の行動は、世界中の私たちのすべてを脅かすことになるのです。

グローバル暗号化デーに際し、私たちは政府および民間セクターに対し、暗号化を弱体化させるような取り組みを拒否し、代わりに、世界中の人々を守るために強力な暗号化の使用を促進し、強化する政策を推進するよう呼びかけます。また、私たちは、強力な暗号化を自社のサービスやプラットフォームに導入することで顧客を保護しようとする企業の取り組みを支援し、奨励します。

強力な暗号化は、私たちすべてにとってより安全な世界を実現するための重要なツールです。 https://www.jca.apc.org/jca-net/ja/node/407

暗号化：その社会の仕組みとの関わり

実は暗号化への関心はあまり高くはありません。特に、ネットでのコミュニケーションやパソコンでの日常の作業で、暗号化を強く意識して、プライバシーやセキュリティに配慮することを最優先に考えてサービスなどを選択するよりも、安価（あるいは無料）であること、技術的に難しくなく、すぐに使いこなせること、便利なこと、といった要素が選択基準になっている場合が多いと思います。

人々がセキュリティやプライバシーを真剣に考えるのは、実際に被害を被った後でのことになりがちです。つまり手遅れになってから、対処を検討しはじめる、ということになりがちです。

他方で、政府や通信事業者などが、プライバシーやセキュリティへの注意喚起を頻繁に行なってもいます。政府や企業が私たちひとりひとりのプライバシーや通信のセキュリティを最も大切な人権として、最優先事項とみなして対処しているでしょうか。政府や企業が最優先にしているのは、国家の安全保障であったり企業の収益であり、プライバシーではありません。私たちのプライバシーが国家安全保障や企業の利益と対立することがあるのです。反政府運動の活動家や政権の腐敗を調査するジャーナリストの行動は、権力基盤を揺がしかねないた

暗号化：その社会の仕組みとの関わり

めに、政府は、こうした人たちを監視しようとしてきました。政府は、監視のために、通信のプライバシーを侵害して、その内容を把握できるような様々な制度を構築してきました。本来であれば、私たちのプライバシーの権利は、まさに、このような権力による監視や介入の可能性がある場合にこそ、きちんと守られるべき権利でなければならないはずです。多くの人達は反政府活動家でもなければ、ジャーナリストでもないから、上の例は他人事でしかないかもしれません。しかし、そうであっても、実は上の例は「他人事」ではないのです。もし、政府の厳しい監視によって、自由な発言や、政府の腐敗が隠蔽されたままであったとすれば、人々は、ごく少数の人達が提起しようとする議論や情報に接することができません。結果として、自分たちが生きている社会を誤って「自由な社会」と誤解したまま既存の権力を受け入れてしまうかもしれません。

ジャーナリストが取材の過程で様々な人達とコンタクトをとり情報を収集する活動が可能なのは、こうした取材が、第三者による監視に晒されることなく、当事者だけの関係（会話やメールなど）のなかで行なわれるからこそ、率直で隠し事のない真実を語る環境が可能になる

暗号化：その社会の仕組みとの関わり

のです。この環境があってこそ、不特定多数の人達に政府批判の記事も可能になります。この記事を読んだ人達は、自分達の知らなかった事実に接することによって、政府への評価を変えて、従来よりもより批判的な立場をとるかもしれません。このような世論の変化は、政権にとって、より強固な権力の基盤を形成することになるでしょうか。むしろ、逆に、政権の基盤を揺がしかねない事態へと向う可能性が以前よりも高くなるといえそうです。

つまり、ジャーナリストたちが、政府が知りえないところで、密かに情報を収集し取材することは、政府の権力維持目的に寄与するとは限らないのです。むしろ政府にとっては、プライバシーで保護されたジャーナリストの取材活動を監視することの方が権力の維持に役に立つと考えがちなのです。法律でプライバシーや通信の秘密が明記されていても、政府がこの規範を率先して守る動機があるとはいえないのです。政府にプライバシーの権利を保護するように行動させられるかどうかは、私たちの行動にかかっています。

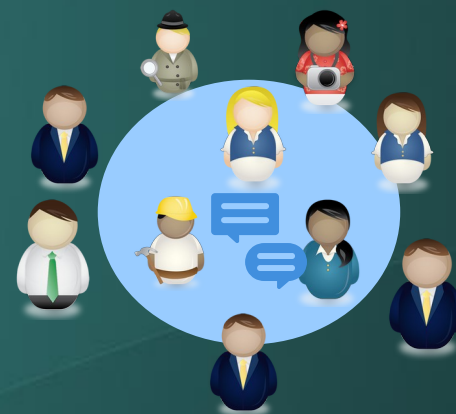
では、こうしたプライバシーの権利を実際に通信（コミュニケーション）で確保するにはどうしたらいいのでしょうか。政府の内部にいる

暗号化：その社会の仕組みとの関わり

人が政権の腐敗について内部告発をしたい、と考えて、ジャーナリストに接触を試みたい、と思ったとします。もし、あなたが、この内部告発者であったら、どのような手段をとるでしょうか。実際にあった有名なケースは、エドワード・スノーデンによる内部告発でしょう。スノーデンは、慎重に信頼できるジャーナリストを選び、相互の通信を暗号化されたメッセージのやりとりにすることで、自分の行動を隠し、内部告発が事前に漏洩しない工夫をしました。暗号化という技術を使うことなしではスノーデンの暴露は成功しなかったかもしれません。

暗号化は、ジャーナリストの取材と記事の作成全体の流れのなかのごく一部に過ぎません。しかし、この暗号化がなければ、取材は制限され、記事も書くことができず、更には、内部告発者はより容易に摘発されるリスクを負う可能性が高くなることは確実でしょう。

内部告発者とジャーナリストという例はかなり古典的な枠組みのようにみえますが、例示をもう少し身近なケースにして考えることもできます。たとえば、学校での教師のハラスメントや家庭内のドメスティック・バイオレンスといった出来事の被害者が、外部に助けを求

暗号化：その社会の仕組みとの関わり

める場合、加害者に知られることなく外部の支援者と連絡をとる手段として、暗号化されたメッセージのやりとりは不可欠です。

反政府運動の活動家にとっても、プライバシーの権利は重要な言論の自由の前提です。上の左図は、いわゆる「原っぱモデル」です。周囲に誰もいない場所で、活動家たちがデモの準備のための議論をしていると想像してみてください。上の右図は、周囲に多くの人達がいるなかで相談するシチュエーションです。言論の自由が保障されている、という建前を文字どおりに受け取れば、どちらの場合も、活動家たち

暗号化：その社会の仕組みとの関わり

の議論に影響を及ぼさない、ということになるでしょう。しかし、多くの場合、権力に抗う人達は、最初は少数であるのが常です。（ずっと少数かもしれませんが）周囲には政権を支持する人達に囲まれることになります。こうしたなかで、果して率直な議論ができるでしょうか。反政府運動の行動はいちはやく政府に察知されるでしょう。政府はこうした行動を言論の自由の権利行使として、歓迎するでしょうか。それとも、可能な手段を使って抑え込もうとするでしょうか。政府が弾圧にでたとき、右図の周囲にいる人達がどのような行動をとるでしょうか。どのようになるのかは、一概には結論を出せませんが、少なくとも、周囲で議論を聞いている不特定多数の人々がいるなかでの自由な議論は制約を受けるとみてよいでしょう。

このように社会の少数者が自由に議論をすることができるためには、対立する多数者からの干渉を受けない環境が必要であり、プライバシーの権利がこのような自由な環境を保障する権利になります。とはいえ、権利が具体化できなければならず、「原っぱ」

暗号化：その社会の仕組みとの関わり

のような環境が通信環境で実現できなければなりません。

暗号化によって人々が自由に議論し、政府への批判を行動に移すことができれば、社会のなかに、既存の政権や支配的な考え方とは異なる考え方をもつ人々がいることを、多くの人々に気づいてもらえることになります。このようなコミュニケーションの状況を実際に実現するための技術が暗号化技術になります。もし、「原っぱ」モデルのような条件が通信環境で実現できなければ、社会は、既存の権力の支配の腐敗にも気づかないまま、その支配を受け入れてしまうかもしれません。言論だけで社会や政治を変えることはできませんが、自由な議論は社会や政治を変えるための必要条件なのです。

暗号化：その社会の仕組みとの関わり

私たちにとってのコミュニケーションの基本は以下のようになります。

- コミュニケーションは、私が中心にあって成り立っているわけではない。コミュニケーションとは「誰か」とのコミュニケーションです。この「誰」こそが主役です。
- この「誰」が目の前にいようが遠く離れた場所にいようが、コミュニケーションの権利に差があってはなりません。
- コミュニケーションのプライバシーは相手と自分のプライバシーが表裏一体のものとして成り立つものです。
- 社会には支配的な価値観と少数者（ジェンダー、国籍など）の文化や価値観の対立や食い違いが必ずあります。このなかで、自由とは、少数者の自由を意味する、と考えておく必要があります。
- 社会の多数者も少数者の言論・表現に影響され触発されることで社会全体が変ります。このきっかけの小さな「種」は、原っぱモデルのようなプライバシーで保護された自由なコミュニケーション（対話や議論）にあります。

暗号化：その社会の仕組みとの関わり

この基本に対して政府や企業は私たちとは異なる利害関係をもちます。

- 政治権力が目指すのは、より強固な権力基盤の構築であり、自らの権力が脆弱になったり、別の政権に交代することを歓迎しません。
- コミュニケーションは民主主義の基本であり、代議制を支える基本です。
- 上の二つの条件を重ね合わせると、コミュニケーションを通じて、より強固な権力基盤を構築する仕組みが、社会のなかに生まれるだろう、ということがわかります。
- 権力にとって、個人のプライバシーの権利よりも権力の維持（や拡大）が優先されます。プライバシーを優先した結果として、権力が脆弱になるような法制度を極力回避しようとします。
- 権力を脆弱にするようなプライバシーへの保護よりも、人々が何を考えているのか、政府に対してどのような異論や抗議の行動をとろうとしているのかなど、権力を揺がしかねない言動を監視しようとします。プライバシーの権利を権力に期待できるとは限らないのです。

暗号化：その社会の仕組みとの関わり

- 企業は、収益を目的とする組織体です。コミュニケーションのプライバシーもこの収益との兼ね合いで、その保護のありかたが決まります。
- 市場経済では、買い手が何をいくらで買うかを決めます。押し売りはできません。しかも、売り手にとって買い手が実際に買ってくれるのかを事前に予測することは困難であり、そもそも何者なのかを知ることも容易ではありません。
- 上の二つの条件から、企業は収益を確実にするためには、買い手の個人情報をより多く収集して、買い手が何を欲がっているのかを探ることに関心を持ちます。
- 人々の日常生活のプライバシーは、市場での購買行動と不可分です。いつ、どこで、何を、どのような目的で購入したのか、こうした行動は「嘘」や「騙し」ではない正直な自分の関心や欲望の結果ですから、自分の本当の姿を晒しやすくなります。

暗号化：その社会の仕組みとの関わり

- 企業にとって個人のプライバシーを知ることは、収益に繋がるものです。だから、プライバシー情報を取得したがることになります。
- 市場経済では、プライバシーは容易に「商品」化され売買対象になります。この情報が収益に繋がるので欲しいけれども入手が困難だからです。
- 他方で、プライバシーを守りたいという需要も生まれ、この需要を満たすサービスもまたビジネスになります。
- 市場は本質的にプライバシー保護を目的とする仕組みではありません。あくまで収益の手段にすぎません。プライバシー保護のビジネスは、収益が得られなくなれば打ち切られます。

暗号化：その社会の仕組みとの関わり

以上のようなプライバシーをめぐる社会の仕組みのなかで、私たちひとりひとりの行動がプライバシーをより強固なものにできるかどうかの鍵を握ることになります。

- 政府にも企業にも、その性質上プライバシーの権利を保護する動機に関して、大きな限界があります。
- しかし、私たちがプライバシーの権利のために、政府や企業の動機の限界に挑戦することで、この限界を一定程度解除することが可能です。
- 逆に何も行動しなければ、政府も企業もその動機に基いてしか行動しないでしょう。政府はより強固な権力基盤のために、企業はより高い収益のために、私たちのプライバシー情報やプライバシー環境を自分たちの目的達成の手段として利用するだけになります。

私たちがプライバシーの権利のために行動すると政府や企業の利害と対立し、様々な逆風に晒されるのは以上のような理由によるのです。

暗号化：その社会の仕組みとの関わり

ですから、私たちにとっての課題は、政府や企業とは別に、私たちが自分の判断で自分のコミュニケーション環境のプライバシーやセキュリティを考えてどう行動するかにかかってきます。もちろん、政府や企業のサービスを完全に無視して実践することは不可能です。政府や企業がプライバシーの権利に好ましい対応をするよう促し、実際にそうした傾向をもつものを更に支持しつつ権利を守る枠組みを構築することが必要になります。

コンピュータに関わるコミュニケーションは、技術的に難解で複雑でもあり、誰もがわかるものではありません。そのために、個人としての努力は勿論のことですが、この分野でテクノロジーに関心をもって活動する組織や団体の果す役割はとても重要になります。

- 人々にとってのプライバシーやセキュリティが、政府や企業のいう意味でのそれらとどこが違うのかなど、基本的な考え方の違いを明確に指摘することような組織が存在すること
- コンピュータを巡る様々なトラブルや疑問を政府や企業のサポートに委ねるのではなく、人々が相互に協力して解決できるような環境を作り、プライバシーを最優先とする技術開発を促すこと

が大切になります。

暗号化：その社会の仕組みとの関わり

暗号化というテーマのためにかなり回り道をしました。しかし、この回り道は、私たちが、プライバシーの権利を自分のこととして、また、それ以上に私が関わるコミュニケーションの相手の「誰か」のこととして理解する上で必須の回り道です。

コミュニケーションにおけるプライバシーの権利をきちんと確保しようとするならば、そのために必要な手立てを自分が主体となって工夫することが重要になります。プライバシー情報を取得したがる政府や企業に委ねることが最善の方法にはなりません。

自分と意図した相手との間で自由なコミュニケーションを邪魔されたり覗かれたりせずに実現するために、特に遠隔地とのコミュニケーションに不可欠な技術が暗号化になります。暗号化によって、私たちは上で述べたような、自由に考え、意見を表明し、議論し、行動するためのコミュニケーションの枠組みが可能になります。私に直接関係しない少数者の人達にこうした枠組みが保障されることが大切である、それなしに、私がこの社会で自由であることはできないということは先にも述べた通りです。

以下は、暗号化のための具体的な方策の一例の紹介になります。

暗号化：私の場合はどうなのか

	私が使っている暗号化の手段	一般的に普及している暗号化されていないサービスなど	私が使っていない暗号化の手段
メール	Proton、 Tuta、 PGP (Tuta のみ件名も暗号化)	Gmai 、 Yahoo mail 、または nifty 、 docomo など	Mailbox.org、 Runboxなど
ファイル	Veracrypt CryptPad 、 ProtonDocs	GoogleDocs	注参照
メッセージングアプリ	Signal 、 Telegram	Line(秘密のトークの場合のみ E2EE) 、 Slack 、 WeChat	Threema、 Elementなど
デバイス	ハードディスク全体の暗号化 (Linux)	市販の Windows や Mac 、あるいは通常の方法での Linux のインストール	

(注)Researchers Ðiscover Severe Security Flaws in Major E2EE Cloud Storage Providers (研究者、主要な E2EE クラウドストレージプロバイダーに深刻なセキュリティ欠陥を発見)

上記の表は私の場合であって、一般化して考えないでください。人それぞれ最適な選択があるはず。私の選択も私にとってベストとは考えていません。まだ検討の余地があります。

E2EE メール
サービスの例

https://www.techradar.com/best/best-secure-email-providers

Quick overview

Email Provider Name:	Runbox	ProtonMail	Mailbox.org	Tuta	Sta
Encryption	PGP (with addon)	PGP	PGP	Hybrid AES + RSA	PG
Jurisdiction	Norway (14 Eyes)	Switzerland	Germany (14 Eyes)	Germany (14 Eyes)	N (9
Open Source	Client Apps Only	Yes	No	Client Apps Only	N
Custom domain	Yes (Micro plan)	Yes (Plus plan)	Yes (Standard plan)	Yes (Premium plan)	Ye (D pl
Aliases	Yes (paid)	Yes (paid)	Yes (paid)	Yes (paid)	Ye
Mail client support	Yes (IMAP, POP, SMTP)	Yes, but through Bridge	Yes (IMAP, POP3)	No	Ye SM
Security audit	No	Yes (2021, by Securitum)	German BSI	Apparently, but not published	Ap bu pu
Accepts crypto payments	Yes (BTC only)	Yes (BTC only)	No	No (But ProxyStore gift cards accepted	Ye or or pe ac
Pricing (lowest)	$1.66	Free (1 GB max storage)	€1	Free (1 GB max storage)	€3

メールの暗号化

最も簡単な方法：暗号化メールサービスを使う

- Proton https://proton.me/mail
- tuta https://tuta.com/ja

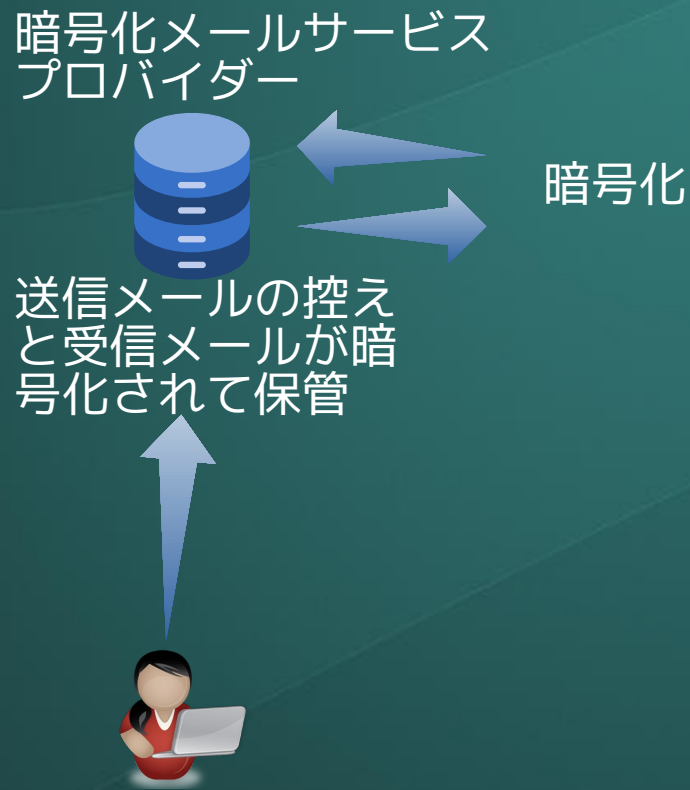
何ができるのか

- メールの送信者と受信者の双方が同じ暗号化メールサービスを使っている場合、エンド・ツー・エンド暗号化が可能
- 送信者が proton や tuta を使い、受信者が一般的なメールサービス(例えば Gmail など)を使っている場合も共通の秘密のパスフレーズを共有するか公開鍵暗号(GPG など)を使えば可能
- メールアカウントの取得は比較的容易。無料から始めて、気に入れば有料契約にして本格的に使うことができる。
- proton はカレンダー、データの保管などの機能があり、 tuta にはカレンダーの機能がある。
- proton や tuta などでグループメール機能を使えばメーリングリストも E2EE になるが全員が proton や tuta を使う必要がある。

メールの暗号化

暗号化メールサービスプロバイダー

暗号化

送信メールの控えと受信メールが暗号化されて保管

暗号化メールサービスを使うメリットは単にメッセージを暗号化して送受信できることに加えて、

- 送受信は暗号化サービス業者のサーバーを用いるので、自分のパソコンにデータを残さない
- 送信控えと受信メールは暗号化サービス業者のサーバーに暗号化されて蓄積される
- これらのメッセージ本文は業者でも読むことができない

秘匿性の高いメッセージングアプリ

Signal

https://signal.org/ja/

Telegram

https://telegram.org/

いずれもスマートフォンにインストールして使う。スマホにインストールした後でデスクトップパソコンとも連携することが可能だ。

インストールを Google Play や Apple Store から行なうのであれば、ワンクリックでインストールが完了する。しかし、これらのサイトを使わないでインストールするには若干の作業が必要になる。たとえば Telegram の場合については下記を参照

https://telegram.org/android

(注)Android であれば、 Google Play を使わないでインストールすることが可能。 APK ファイルをダウンロードしてインストールする。または Telegram なら F-Ðroidからインストールできるが Signal は F-Ðroid からはインストールできない。

秘匿性の高いメッセージングアプリ

（参考）

(tuta)2024年版WhatsAppの代替案 | プライベートの時間！

https://tuta.com/ja/blog/best-whatsapp-alternatives-privacy

Signal、Telegramの他に下記が紹介されている。

- **Threema** android iOS デスクトップ

  F-Ðroidからインストール可、アプリ有料(1000円)、電話番号不要、メアド認証、Lineからの移行も多いかも

- **Element** android iOS デスクトップ

  F-Ðroidからインストール可、メアド認証が必要

- **Wire** android iOS
- **SimpleX** android iOS desktop
- **Session** デスクトップとモバイル

など

いずれについても、長所と短所が列記されている。

PROVIDER	Open Source	E2E Encryption	Security Audits	Encrypted Video Calling	Anonymous
Signal	✓	✓	✓	✓	✗
Threema	✓	✓	✓	✓	✓
Wire	✓	✓	✓	✓	✗
Element	✓	✓	✗	✓	✓
SimpleX	✓	✓	✓	✓	✓
Session	✓	✓	✓	✓	✓

表WhatsAppに代わるセキュアメッセージングアプリのセキュリティと機能比較:Signal, Threema, Telegram, Element, Wire, SimpleX, Session.

ファイルの暗号化

ファイル暗号化サービスを使う

- Cryptpad https://cryptpad.fr/

  JCA-NET セミナーでの解説

  https://pilot.jca.apc.org/nextcloud/index.php/s/J6aRkHmRĐfQG59i
- Proton にはドキュメント保存サービスがある

ファイル暗号化のソフトウェアを導入する。たとえば

- Veracrypt

  https://www.veracrypt.fr/code/VeraCrypt/

  https://www.gigafree.net/security/encrypt/VeraCrypt.html

ファイルの暗号化

たぶん最も簡単な方法は、エンド・ツーエンド暗号化に対応しただデータ保存サービスを使うことだろう。

Crypt Pad や Proton のサービスを使えば、データを暗号化したまま保存することができる。自分のパソコンなどに保存する場合と比べて

- ノートパソコンの紛失などでデータ流出が防げる
- 暗号化に対応していないサービスの場合はサーバー側で盗み見されたり第三者に取得される恐れがある
- 安全に特定の相手にデータを送るための手段として使える

Google Docs v.s. Proton Docs

参考

Google Docs はもうお役御免？ Proton Docs を検討すべき理由 (Life Hacker ジャパン)

https://www.lifehacker.jp/article/2407-why-you-should-consider-proton-docs-over-google/

Google と Proton のストレージサービスを比較した記事

「 Google はクラウド上でデータを保存する際に独自の暗号化を利用しています。しかし、 Google の場合、完全にエンドツーエンドで暗号化されていないため、 Google はユーザーのデータにオープンアクセスすることが可能。 Google は生成型AIを「公にアクセス可能な」情報でのみトレーニングすると説明しています。これは多くの人にとって影響を与えるものではないですが、特に Smart Compose などの AI をはじめとした機能については例外を設けており、一部の人にとって弱点として見られる部分でしょう。このような懸念から、最近ではエンドツーエンドの暗号化を備えた製品が非常に重要視されるようになっています。」

Google Ðocs v.s. Proton Ðocs

参考

Google Ðocs はもうお役御免？ Proton Ðocs を検討すべき理由 (Life Hacker ジャパン)

https://www.lifehacker.jp/article/2407-why-you-should-consider-proton-docs-over-google/

「 Proton Ðocs には、ほかのテキストエディタ、特に Google ドキュメントと一線を画す大きな特徴があります。それは「エンドツーエンドの暗号化」です。

Proton は「プライバシーの保護が第一」をモットーに掲げて事業を展開しており、その考え方は最新のソフトウェア提供にも適用されています。

Proton Ðocs は、カーソルの動きに至るまでエンドツーエンドで暗号化されており、 Proton を含め誰もがドキュメントで何をしているか追跡できません。ドキュメントは Proton のサーバーに到達する前にロックされます。」

Proton Ðocs v.s. CryptPad

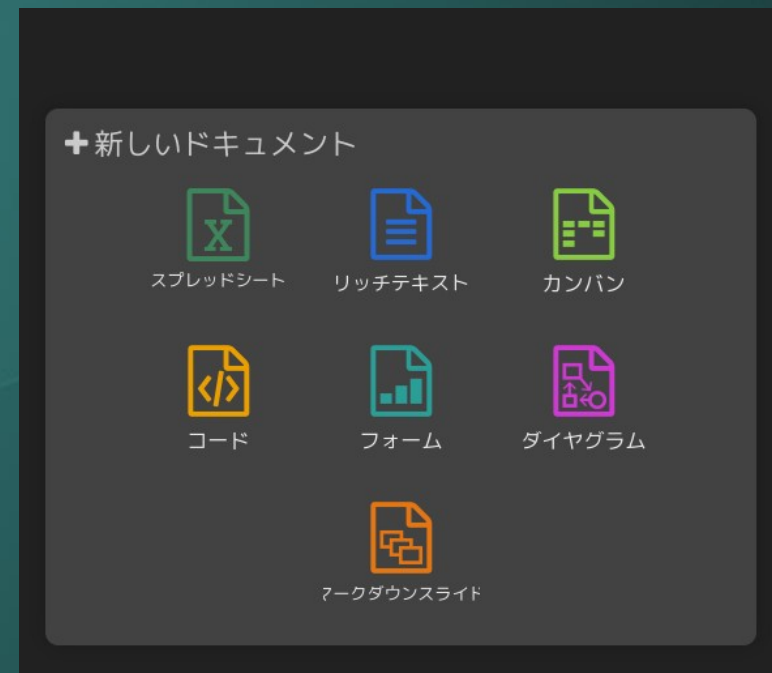
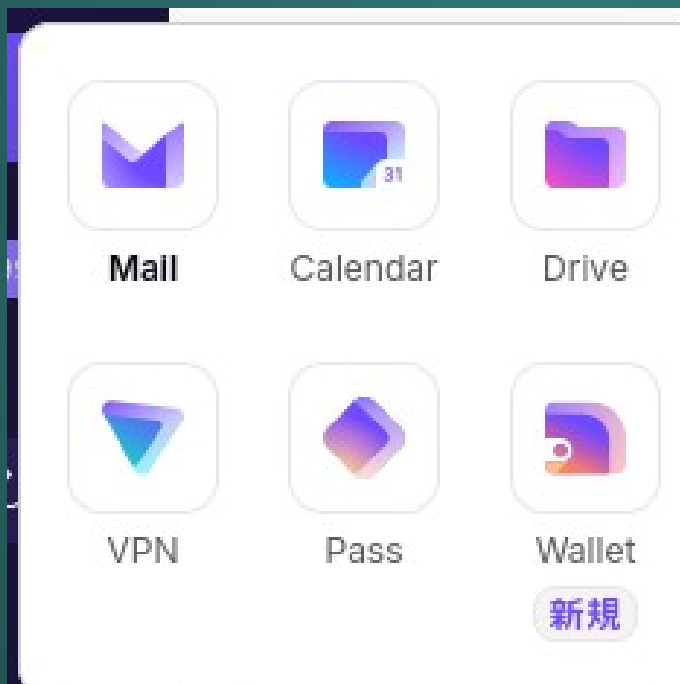
どちらもE2EE暗号化を提供しているが、CryptPadのほうが提供しているサービスの種類が多様だ。

「エンド・ツー・エンド暗号化(e2ee)サービスには、メッセージング(例：Signal)、個人用メモ(共同作業なし、例：Joplin)、文書ストレージ(編集なし、例：Proton Ðrive)に特化したものがある。しかし、e2ee + 文書編集 + リアルタイム共同作業のベン図に当てはまる製品は実際には多くない。」

参考

CryptPad、安全なデジタルコラボレーションにおけるアクセシビリティとプライバシーのバランスについて

https://www.jca.apc.org/jca-net/ja/node/408

Proton Docs v.s. CryptPad

右が CryptPad 、左が Proton 。 CryptPad にはメールや VPN のサービスがないが、文書、表計算、フォームの作成などがある。両方をうまく使い分けるのでもいいかもしれない。なお tuta はメールとカレンダーのみしか提供していないが、件名も暗号化してくれるのは他にはないメリットかも。、また、メールサービスであっても、重要な文書をメールの添付書類として自分の tuta のアカウントに送信して tuta のサーバーに保管する、という方法でドキュメント保存の代用にすることができる。

強固な暗号化サービスであっても パスワード管理が杜撰ならアウト！

Proton や Tuta のメールサービスにアクセスするためには、パスワードでログインします。スマホで Signal を使う場合も、ログインパスワードを使います。パスワード利用は必須の条件です。

もしパスワードを使い回ししていたり、生年月日や容易に推測可能な安易な文字列を用いてパスワードを破られてしまえば、どんなに強固な暗号化サービスも意味をなしません。

E2EE の強固な暗号化サービスを利用するための大前提は、パスワードの原則（推測されない、長い文字列、使い回しをしないなど）をきちんと守る必要があります。

やれるところから
自分のライフスタイルに

暗号化は、技術的な知識なしに導入できるものが多くあります。しかし他方で、導入する「壁」になるのは、これまで自分が慣れ親しんだソフトウェアやサービスを捨てて新しい環境に移行するための段取りに踏み切る決断ができるかどうか、になります。

このときに、「暗号化」がプライバシーやコミュニケーションの私たち皆の権利にとっての重要性を再認識しつつ、無理のない範囲で移行を進めることを是非検討してください。

わからないことがあれば、遠慮なく相談してください。